УДК 004.85:004.832.2

ИСПОЛЬЗОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ МНОГОЭТАПНЫХ КИБЕРАТАК НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

Сизов А. И.[1], Тельбух В.В.[1]
Научный руководитель – канд. техн. наук, преподаватель Тельбух В. В.[1]
[1]Военно-космическая академия имени А.Ф. Можайского

Введение

Цифровая инфраструктура растёт и усложняется. Системы распределены, сервисов много, учетных записей ещё больше. Каждый день в сеть входят сотрудники, подрядчики, сервисные боты. Поток событий огромный. На этом фоне злоумышленники действуют тихо. Они не ломают двери — они входят как свои. Классические инструменты защиты ловят известные сценарии. Они опираются на сигнатуры, заранее заданные правила и шаблоны атак. Если схема новая или растянута во времени, сигнал может появиться слишком поздно. Многоэтапные вторжения часто маскируются под обычные действия пользователя. Внешне всё выглядит нормально. Ущерб уже нанесён, а тревога только поднимается. Отсюда интерес к поведенческой аналитике. Она не ищет конкретный вредоносный код. Она наблюдает за действиями: когда пользователь входит в систему, какие ресурсы открывает, как перемещается между сервисами. Из этих деталей складывается цифровой портрет. [1, 2].

Основная часть

Именно на этой идее строится подход UEBA (User and Entity Behavior Analytics) — анализ поведения пользователей и сущностей. Система учится понимать норму. Затем она замечает отклонения, даже небольшие. Для реализации такого подхода обычно используют SIEM или XDR-платформы. Они собирают журналы событий, связывают их и показывают общую картину. Проблема в том, что доступ к значительной части решений ограничен ввиду их коммерческого характера. Настройка под учебные проекты или исследовательские задачи требует ресурсов и лицензий. Это тормозит эксперименты и внедрение в университетской среде, поэтому внимание всё чаще смещается к открытым инструментам. Они гибкие, их можно адаптировать под конкретную инфраструктуру и на их базе проще строить собственные модели машинного обучения. [3, 4].

В качестве основы будем использовать open-source платформу Wazuh. Она собирает журналы событий, отслеживает активность учетных записей и фиксирует изменения в системе. Платформа умеет коррелировать события безопасности и выводить их в единую панель. Это удобный фундамент для анализа поведения. [5].

Предлагаемый подход строится вокруг нескольких шагов:

1. Сбор и очистка данных.

Сначала настраивают централизованный сбор логов:

– события входа и выхода из системы;
– сетевые обращения;
– действия пользователей и сервисных аккаунтов.

Поток данных приводят к единому формату. Удаляют дубликаты. Объединяют события в сессии. На этом этапе важна точность. Грязные данные ведут к ложным выводам. [5].

2. Построение поведенческих профилей.

Когда база накоплена, формируются характеристики обычной активности. Система фиксирует:

– время работы пользователя;
– типичные ресурсы;
– частоту обращений;

– объёмы передаваемой информации.

Так появляется модель «нормы». У каждого пользователя она своя. У разработчика — одна, у администратора — другая. [3].

3. Применение машинного обучения.

Далее подключаются алгоритмы без учителя. Они не требуют размеченных атак. Модель анализирует данные и ищет отклонения от привычного поведения. Если сотрудник внезапно начинает выгружать большие объёмы данных ночью или обращается к нетипичным серверам, система это замечает, даже если сигнатуры атаки нет. Подход даёт гибкость. Он позволяет обнаруживать угрозы, которые ещё не описаны в базах. [3].

4. Оценка риска.

Каждому событию присваивается риск-балл. Он растёт, если действия выходят за рамки обычного профиля. При достижении порога система отправляет уведомление или запускает реакцию. Сначала — аналитикам. Затем можно подключить автоматические сценарии: блокировку сессии, временное ограничение доступа. Внедрение лучше проводить постепенно. Сначала система работает в режиме наблюдения. Она собирает данные и обучается. Затем появляются уведомления для специалистов. И только после этого можно переходить к автоматическим действиям при критических отклонениях. [5].

Подход даёт заметные преимущества:

– основан на открытой платформе, доступной для исследований;
– обнаруживает неизвестные сценарии атак;
– реагирует на ранних стадиях;
– снижает нагрузку на аналитиков за счёт приоритизации событий;
– масштабируется под инфраструктуру организации;
– интегрируется в существующие центры мониторинга безопасности.

Выводы

Данная технология открывает простор для исследований. Необходимо улучшать интерпретируемость моделей, уменьшать ложные тревоги, учиться переносить алгоритмы между организациями без утечки данных. Для молодых учёных это богатое поле работы. Поведенческий анализ меняет сам подход к защите. Он делает акцент на раннем сигнале. Машинное обучение превращает поток логов в систему предупреждений. Чем раньше обнаружено отклонение, тем меньше риск для инфраструктуры и тем выше устойчивость цифровой среды.

Литература

1. Kaspersky. Отчёт о современных киберугрозах [Электронный ресурс]. — URL: https://www.kaspersky.ru (дата обращения: 22.01.2026).
2. Positive Technologies. Ландшафт киберугроз [Электронный ресурс]. — URL: https://www.ptsecurity.com (дата обращения: 27.01.2026).
3. Security Vision. UEBA: поведенческий анализ пользователей [Электронный ресурс]. — URL: https://www.securityvision.ru (дата обращения: 30.01.2026).
4. Cloud Networks. UEBA-подход к анализу поведения пользователей [Электронный ресурс]. — URL: https://cloudnetworks.ru (дата обращения: 30.01.2026).
5. Wazuh. Open Source Security Platform [Электронный ресурс]. — URL: https://documentation.wazuh.com (дата обращения: 10.02.2026).